

MRM:MEF
F.# 2020R00016

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
TWITTER PROFILES WITH USERNAMES
(1) @BINGIEBONGIE AT
HTTPS://TWITTER.COM/BINGIEBONGIE;
(2) @THELIFEOFCHRIS88 AT
HTTPS://TWITTER.COM/THELIFEOFCHRIS88;
(3) @LIFEOFCHRIS69 AT
HTTPS://TWITTER.COM/LIFEOFCHRIS69;
(4) @DACRYPHLLIC AT
HTTPS://TWITTER.COM/DACRYPHLLIC;
(5) @SOMNOPHLLIC AT
HTTPS://TWITTER.COM/DACRYPHLLIC;
AND (6) @DACRYYYBOYY AT
HTTPS://TWITTER.COM/DACRYYYBOYY,
THAT ARE STORED AT PREMISES
CONTROLLED BY TWITTER

**APPLICATION FOR A
SEARCH WARRANT FOR
INFORMATION IN
POSSESSION OF A PROVIDER
(TWITTER ACCOUNTS)**

No. 21-MJ-210(ARL)

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, AARON E. SPIVACK, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Twitter account that is stored at premises owned, maintained, controlled, or operated by Twitter, a social-networking company headquartered in San Francisco, CA. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a

search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Twitter to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Twitter account.

2. I am a Special Agent with the FBI. As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the FBI for approximately 12 years. I am now assigned to the FBI’s Child Exploitation and Human Trafficking Task Force, which investigates individuals suspected of being involved in the receipt, distribution, possession and production of child pornography and sex trafficking, among other offenses. While employed by the FBI, I have conducted and participated in numerous investigations of criminal activity, including, but not limited to investigations related to the sexual exploitation of children, child pornography, and other sex offenses. As a result, and based on my training and experience, I am familiar with the laws regarding sexual offenses and how sexual offenses are commonly committed. I have been assigned to investigate violations of criminal law relating to sexual offenses, and I have gained expertise in how to conduct such investigations through, among other things, training I have received in seminars and classes, and my daily work in relation to these types of investigations. As part of my responsibilities, I have participated in numerous investigations into the commission of various sex offenses. During these investigations, I have executed, or participated in the execution of, numerous search warrants involving electronic devices. I have also received training regarding computer technology and the way electronic devices

are used to further criminal activity, including sex offenses. I have training and experience in numerous areas of criminal investigations and procedures, including search warrant applications, executing searches and seizures, and seizing and processing computer evidence. As part of my responsibilities, I have reviewed thousands of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that CARMINE SIMPSON violated Sections 2251 (sexual exploitation of children), 2252 (transportation, receipt, distribution and possession of material involving sexual exploitation of minors), 2252A (transportation, receipt, distribution and possession of child pornography) and 2422 (coercion and enticement) (together, the “Subject Offenses”). There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

DEFINITIONS

For the purposes of this affidavit, the following terms have the indicated meaning herein:

a. “Child Pornography,” as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

b. “Child Erotica,” as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.

c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]”

e. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, drives, or electronic notebooks and tablets, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

PROBABLE CAUSE

5. On or about December 30, 2020, law enforcement in Maryland received two cybertips from the National Center for Missing and Exploited Children (“NCMEC”), informing them that an individual (the “TARGET”) was utilizing a Twitter account with the number 1240754153749692416 (the “TARGET ACCOUNT”) to communicate with and persuade minors to produce and send sexually explicit images and videos to him (together,

the “Reports”). According to records submitted by Twitter in connection with the Reports (the “Twitter Records”), the TARGET ACCOUNT is associated with the following vanity names: (1) “@BINGIEBONGIE”, (2) “@thelifeofchris88”, (3) “@LifeOfChris69”, (4) “@DACRYPHILIC”, (5) “@SOMNOPHLLIC” and (6) “@DACRYYYBOYY”.

Additionally, the profile associated with at least one of these vanity names included an age for the TARGET of 17 years old.

6. Based on the Twitter Records, the TARGET had a cellular telephone with a number ending in 2276 (the “2276 Number”). According to the same records, the TARGET ACCOUNT was created on March 19, 2020 and suspended by Twitter on or about December 31, 2020.

7. Based on the Twitter Records, which include online chats occurring in or about and between April 2020 and December 2020, the TARGET communicated with at least 46 apparent minors, who appear to have been between the ages of 13 and 17. In these chats, the TARGET requested that the minors take sexually explicit videos and pictures of themselves, oftentimes masturbating or after drawing on their body with a marker. Based on a review of the material submitted by Twitter, the TARGET obtained at least 18 photographic images and 33 videos containing apparent child exploitative material from minors. The TARGET also obtained at least 162 photographic images and 48 videos containing child erotica. During these conversations, the TARGET repeatedly represented that he was 17 years old.

8. Included in the Reports and Twitter Records is information regarding various IP addresses used by the TARGET to access the Internet. Using these IP address, in

addition to other information obtained as part of the investigation, the FBI identified the TARGET as CARMINE SIMPSON, who was living at a residence in Holbrook, New York (the “TARGET RESIDENCE”).

9. On January 27, 2021, the FBI obtained a search warrant for the person of CARMINE SIMPSON, the telephone associated with the 2276 Number (the “TARGET PHONE”) and the TARGET RESIDENCE and all electronic devices therein. (21 MJ 115 (currently filed under seal)).

10. Pursuant to that search, the FBI recovered the TARGET PHONE, which is an iPhone, among other devices. A search of the TARGET PHONE revealed numerous photos that SIMPSON had taken of himself and shared on Twitter, using the TARGET ACCOUNT, with the minor victims, including photos of his penis. Additionally, during the search of the TARGET RESIDENCE, the FBI found a pair of boxer shorts that SIMPSON was wearing in photos that he had shared on Twitter while using the TARGET ACCOUNT. Additionally, a review of the TARGET PHONE revealed that SIMPSON had a number of contacts saved in his phone that were labeled to indicate that they corresponded with individuals he met on Twitter. For example, there are contacts in the TARGET PHONE that include “Stefanie Twitter,” “Sophie Twitter,” and “Margaret Twitter.” There are also messages contained in various applications in the TARGET PHONE and other electronic devices seized from the defendant wherein he suggests meeting up with someone that he has apparently met online.

11. Additionally, the government has interviewed an individual who is employed by the NYPD, but is currently on modified duty, who was periodically partnered with

CARMINE SIMPSON in 2019 (“Police Officer 1”).¹ Police Officer 1 stated in substance inter alia that while he was partnered with SIMPSON, SIMPSON repeatedly stated in sum and substance that he was interested in young girls, SIMPSON showed Police Officer 1 photos of nude females, who SIMPSON represented were 13 and 14 years old and who appeared to be pre-pubescent, and SIMPSON further stated in sum and substance that he was having intercourse with the 13-year-old female pictured in one of the photos.

12. On January 28, 2021, CARMINE SIMPSON was placed under arrest and charged by complaint with violating 18 U.S.C. 2251(a) (sexual exploitation of a minor) (No. 21 MJ 119). The complaint is attached hereto as EXHIBIT 1, and is fully incorporated herein.

13. On December 30, 2020, law enforcement submitted a preservation request to Twitter for the TARGET ACCOUNT.

14. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.

¹ Police Officer 1 is currently the subject of an indictment in the Eastern District of New York charging wire fraud, in connection with a scheme to submit fraudulent postal insurance claims. Police Officer 1, with counsel, met with the government pursuant to a proffer agreement and provided information about SIMPSON. No promises have been made to Police Officer 1 in exchange for Police Officer 1 meeting with the government.

15. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

16. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

17. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

18. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

19. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when

the Tweet was posted to Twitter. Twitter users can also “favorite,” “retweet,” or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a “mention” of the identified user. In the “Connect” tab for each account, Twitter provides the user with a list of other users who have “favorited” or “retweeted” the user’s own Tweets, as well as a list of all Tweets that include the user’s username (*i.e.*, a list of all “mentions” and “replies” for that username).

20. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

21. Twitter users can also opt to include location data in their Tweets, which will reveal the users’ locations at the time they post each Tweet. This “Tweet With Location” function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

22. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter’s link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.

23. A Twitter user can “follow” other Twitter users, which means subscribing to those users’ Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user’s “followers” list) and a list of people whom that user follows (*i.e.*, the user’s “following” list). Twitter users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that

their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into “lists” that display on the right side of the user’s home page on Twitter. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

24. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter’s database.

25. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user’s mobile phone, and the user can also set up a “sleep time” during which Twitter updates will not be sent to the user’s phone.

26. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

27. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users’ public Twitter profiles.

28. If a Twitter user does not want to interact with another user on Twitter, the first user can “block” the second user from following his or her account.

29. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter’s terms of service, during which time the Twitter user will be prevented from using Twitter’s services.

30. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user’s account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, communications, “tweets” (status updates) and “tweeted” photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with

the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to “tweeted” communications. This geographic and timeline information may tend to either inculcate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner’s state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

31. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Twitter to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of

Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

33. Based on the forgoing, I request that the Court issue the proposed search warrant.

34. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

36. The government will execute this warrant by serving the warrant on Twitter. Because the warrant will be served on Twitter, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



AARON E. SPIVACK
Special Agent
FEDERAL BUREAU OF
INVESTIGATION

Subscribed and sworn to before
me On February 18, 2021



HONORABLE ARLENE R. LINDSAY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

EXHIBIT 1

MRM:MEF
F. #2021R00016

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----- X

UNITED STATES OF AMERICA

C O M P L A I N T

- against -

(18 U.S.C. § 2251(a))

CARMINE SIMPSON,

No. 21 MJ 119

Defendant.

----- X

EASTERN DISTRICT OF NEW YORK, SS:

AARON E. SPIVACK, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

On or about and between April 2020 and December 2020, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant CARMINE SIMPSON did knowingly and intentionally employ, use, persuade, induce, entice and coerce a minor to engage in sexually explicit conduct for the purpose of producing one or more visual depictions of such conduct, knowing and having reason to know that such visual depictions would be transported and transmitted using any means and facility of interstate and foreign commerce and which would be in and affecting interstate and foreign commerce, which visual depictions were produced and transmitted using materials that had been mailed, shipped and transported in and affecting interstate and foreign commerce by any means, including by computer, and which visual depictions were

actually transported and transmitted using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce.

(Title 18, United States Code, Section 2251(a))

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and I have been in that role for approximately 12 years. I am now assigned to the FBI's Child Exploitation and Human Trafficking Task Force, which investigates individuals suspected of being involved in the receipt, distribution, possession and production of child pornography and sex trafficking, among other offenses. While employed by the FBI, I have conducted and participated in numerous investigations of criminal activity, including, but not limited to investigations related to the sexual exploitation of children, child pornography, and other sex offenses. As a result, and based on my training and experience, I am familiar with the laws regarding sexual offenses and how sexual offenses are commonly committed. I have been assigned to investigate violations of criminal law relating to sexual offenses, and I have gained expertise in how to conduct such investigations through, among other things, training I have received in seminars and classes, and my daily work in relation to these types of investigations. As part of my responsibilities, I have participated in numerous investigations into the commission of various sex offenses. During these investigations, I have executed, or participated in the execution of, numerous search warrants involving

¹ Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

electronic devices. I have also received training regarding computer technology and the way electronic devices are used to further criminal activity, including sex offenses. I have training and experience in numerous areas of criminal investigations and procedures, including search warrant applications, executing searches and seizures, and seizing and processing computer evidence. As part of my responsibilities, I have reviewed thousands of images depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. I am familiar with the facts and circumstances set forth below from my own participation in the investigation, my review of the investigative file, and from my conversations with, and review of reports of, other law enforcement officers and agents involved in the investigation.

DEFINITIONS

3. For the purposes of this complaint, the following terms have the indicated meaning herein:

a. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of

which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

b. “Child Erotica,” as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.

c. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. “Domain name” is a name that identifies an IP address.

PROBABLE CAUSE

4. On or about December 30, 2020, law enforcement in Maryland received two cybertips from the National Center for Missing and Exploited Children (“NCMEC”), informing them that an individual (the “TARGET”) was utilizing a Twitter account with the number 1240754153749692416 (the “Twitter Account”) to communicate with and persuade minors to produce and send sexually explicit images and videos to him (together, the “Reports”). According to records submitted by Twitter in connection with the Reports (the “Twitter Records”), the TARGET utilized several different vanity names on Twitter, including “BINGIEBONGIE”, “thelifeofchris88”, “LifeOfChris69”, “DACRYPHILIC”, “SOMNOPHLLIC” and “DACRYYYBOYY”. Additionally, the profile

associated with at least one of these vanity names included an age for the TARGET of 17 years old.

5. Included in the Reports and Twitter Records is information regarding various IP addresses used by the TARGET to access the Internet. At least two of these IP addresses resolve to an address in Holbrook, New York (the "Residence"), where the defendant CARMINE SIMPSON resides. At least four of these IP addresses resolve to locations at the 75th Precinct of the New York City Police Department ("NYPD") in Brooklyn, New York. Based on records received from the NYPD, SIMPSON is employed as a police officer with the NYPD and works in the 75th Precinct, and he has a personal cellular telephone with a number ending in 2276 (the "2276 Number"). Based on information in the Reports and the Twitter Records, the TARGET provided the 2276 Number when he established the Twitter Account.

6. On January 28, 2021, I executed a search warrant at the Residence, where I met and spoke with the defendant CARMINE SIMPSON, who identified himself to me. Prior to executing that search warrant, I reviewed photographs shared by the TARGET on Twitter, including one of an adult male wearing a NYPD t-shirt. During the execution of that search warrant, the FBI located and photographed various items in the Residence that I had previously seen in photographs shared by the TARGET on Twitter, including but not limited to a pair of boxer shorts, a gun holster and several bed spreads. Additionally, during the same search, I recovered SIMPSON's telephone, which I know is assigned the 2276 Number because I called that number and SIMPSON's telephone rang. Having reviewed photographs shared by the TARGET on Twitter and met SIMPSON in person, I can conclude that SIMPSON is the individual pictured in the photographs shared by the

TARGET on Twitter. In some of these photographs, however, SIMPSON used a filter to make himself appear younger than he is. As a result, there is probable cause to believe that the TARGET is CARMINE SIMPSON.

7. Based on the Twitter Records, which include online chats occurring in or about and between April 2020 and December 2020, the defendant CARMINE SIMPSON communicated with at least 46 apparent minors, who appear to have been between the ages of 13 and 17. In these chats, SIMPSON requested that the minors take sexually explicit videos and pictures of themselves, oftentimes masturbating or after drawing on their body with a marker. Based on a review of the material submitted by Twitter, SIMPSON obtained at least 18 photographic images and 33 videos containing child exploitative material from minors. SIMPSON also obtained at least 162 photographic images and 48 videos containing child erotica. During these conversations, SIMPSON repeatedly represented that he was 17 years old.

8. For example, on or about and between September 7, 2020 and September 30, 2020, both dates being approximate and inclusive, the defendant CARMINE SIMPSON was communicating via Twitter with Jane Doe 1, who appears to be an approximately 13-year-old female. Initially, SIMPSON groomed Jane Doe 1, saying things like, “Babygirl! You are ADORABLE” and “you’re cute to look at.” The conversation gradually escalated, and SIMPSON asked questions such as, “You own cute undies?”, “Yo so turns out imma be home alone for a bit. If you wanna have like FaceTime sex or something???” Initially, Jane Doe 1 responded, “heh um i cant bc i have to like do school stuff :((sorryyy[.]” Thereafter, SIMPSON convinced Jane Doe 1 to send pictures and videos of herself where she is partially clothed. SIMPSON encouraged Jane Doe 1, saying

things like, “This is hot as fuck,” and then sent Jane Doe 1 links to websites as suggestions of the pictures that he would like of Jane Doe 1. SIMPSON also asked Jane Doe 1 if she owned any “toys.” Jane Doe 1 replied that she did not, but she had a “brush.” After Jane Doe 1 and SIMPSON appear to have had a live chat on a separate platform, Jane Doe 1 sent SIMPSON a 12-second video of herself, in which she is inserting a hair brush into and out of her vagina. SIMPSON replied in substance, “Babygirl dont stop,” “Keep the videos coming for me,” and “I love how wet I made tou [sic].” Thereafter, SIMPSON asked Jane Doe 1 if she liked “body writing”. Several days later, after SIMPSON complained that he had not “seen [Jane Doe 1] naked in two days :(”, and Jane Doe 1 responded that she was busy in school, SIMPSON asked Jane Doe 1 for more nudes.

9. Similarly, on or about and between April 11, 2020 and September 15, 2020, both dates being approximate and inclusive, the defendant CARMINE SIMPSON was communicating via Twitter with Jane Doe 2, who appears to be approximately 15-years-old. Initially, SIMPSON groomed Jane Doe 2, saying things like, “You got cute eyes”, and then progressed to asking for “lewd’s.” Later, during a highly sexual conversation, Jane Doe 2 said that she was “wet,” and SIMPSON asked for “proof.” In response, Jane Doe 2 sent a picture of wet underwear. During these conversations, SIMPSON asked Jane Doe 2 to write various words and phrases on her body, and specifically under her belly button, including “use my holes”, “cum”, “whore”, “useless”, “pig”, “desperate”, “babyboy,” “prince” and “anal slut” and then photograph herself. Thereafter, Jane Doe 2 sent a picture and a video depicting the various words written with a marker on Jane Doe 2’s abdomen. On or about April 13, 2020, as part of a highly sexual conversation, SIMPSON said to Jane Doe 2 in substance, “I wanna see your cute little ass bright red from spankings.” In response, Jane

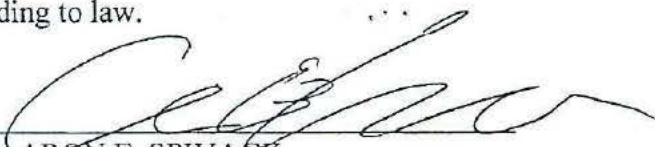
Doe 2 sent a picture of herself, kneeling on a bed, where she is nude from the waist down, her backside is red, and her vagina is visible in between her legs. Later on that same day, SIMPSON asked Jane Doe 2 to “Bend over. Shove your useless face into the bed and spread those cheeks for daddy.” Thereafter, Jane Doe 2 sent a video file depicting herself, lying face down on the ground with her backside up in the air, and her vagina is visible in between her legs. Later that same day, SIMPSON told Jane Doe 2 to “Show me how you fuck yourself Babyboy”, and in response, Jane Doe 2 sent a 25-second video wherein she is inserting her fingers in her vagina from behind. On or about April 23, 2020, after Jane Doe 2 sent SIMPSON a video of herself masturbating, SIMPSON responded, “Try filming it again but this time, put your belt around your neck and pull it.” Thereafter, Jane Doe 2 sent SIMPSON a 36-second video in which Jane Doe 2 is using one hand to pull on a belt to choke herself and the other hand to masturbate. On or about April 25, 2020, SIMPSON told Jane Doe 2 to write “CARMINES SLUTTY LITTLY [sic] BOY” on her chest. Thereafter, Jane Doe 2 asked SIMPSON if that was his name, and SIMPSON responded, “It is. Chris is my middle name” and “I have chris on Cuz 1) Carmine is a weird name 2) it’s rare so I don’t want irl [in real life] to find me.” Jane Doe 2 then sent an image of herself, wherein “CARMINES SLUTTY LITTLE BOY” is written on her chest. In total, it appears that Jane Doe 2 sent SIMPSON approximately 51 files, including photographic images and videos, containing child pornography or child erotica. During the course of communicating with Jane Doe 2, SIMPSON shared his “Snap” username, which he said was “CarmineSimpson.”

Based on a brief search of SIMPSON’s telephone, pursuant to a search warrant executed on January 28, 2021, I observed that defendant had the SnapChat application, which was signed into the “CarmineSimpson” account.

10. Similarly, on or about and between November 19, 2020 and November 20, 2020, both dates being approximate and inclusive, the defendant CARMINE SIMPSON was communicating via Twitter with John Doe 1, an individual whose identity is known to the FBI. John Doe 1 is a transgender male, who was 13 years old on that date. As part of that conversation, SIMPSON said the following, in substance and relevant part: “Do you take good nudes?”, “You take good nudes? Prove it”, “Okay heres what youre gonna do babygirl. Youre gonna grab a sharpie (or a pen) and youre gonna write Im sorry daddy across your tits/chest”, “How many words do you think we can add to your body?”, “Right above your pussy write cum inside me then have an arrow point to your hole”, “Naked in the bathroom?”, “Well do you want to keep taking pictures and videos? Or would you prefer to video call me baby?”, “Well Im [sic] that case I want 4 videos \n1) you slapping your lretty [sic] face \n2) you gagging on your fingers (the more spit the better) \n3) you choking yourself\n4) you pick! Its your choice for number 4,” “Good that can be video #5\nI wanna hear you say my name is [John Doe 1] and my teen body belongs to you,” “Now put on some clothes and get out of there before people start thinking you fell down the toilet”, “Did taking videos for me turn you on?” As part of that conversation, John Doe 1 sent SIMPSON at least two sexually explicit videos. These include a video where John Doe 1 is lying down, fully nude, with marker on their body and their fingers in their vagina.

11. Accordingly, I submit that there is probable cause to believe that the defendant CARMINE SIMPSON used Twitter to persuade minors, including but not limited to Jane Doe 1, Jane Doe 2 and John Doe 1, to create sexually explicit images of themselves and send him these images via Twitter.

WHEREFORE, your deponent respectfully requests that the defendant
CARMINE SIMPSON, be dealt with according to law.


AARON E. SPIVACK
Special Agent, Federal Bureau of Investigation

Sworn to before me this
28th day of January, 2021

/s/ AK Tomlinson
THE HONORABLE A. KATHLEEN TOMLINSON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Twitter profiles with usernames that are stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California:

- (1) @BINGIEBONGIE at <HTTPS://TWITTER.COM/BINGIEBONGIE>;
- (2) @THELIFEOFCHRIS88 at <HTTPS://TWITTER.COM/THELIFEOFCHRIS88>;
- (3) @LIFEOFCHRIS69 at <HTTPS://TWITTER.COM/LIFEOFCHRIS69>;
- (4) @DACRYPHLLIC at <HTTPS://TWITTER.COM/DACRYPHLLIC>;
- (5) @SOMNOPHLLIC at <HTTPS://TWITTER.COM/DACRYPHLLIC>; and
- (6) @DACRYYYBOYY at <HTTPS://TWITTER.COM/DACRYYYBOYY>.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- d. All IP logs and other documents showing the IP address, date, and time of each login to the account;
- e. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- f. All “Tweets” and Direct Messages sent, received, “favorited,” or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;
- g. All information from the “Connect” tab for the account, including all lists of

Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (*i.e.*, “mentions” or “replies”);

- h. All photographs and images in the user gallery for the account;
- i. All location data associated with the account, including all information collected by the “Tweet With Location” service;
- j. All information about the account’s use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- k. All data and information that has been deleted by the user;
- l. A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user’s “following” list and “followers” list);
- m. A list of all users that the account has “unfollowed” or blocked;
- n. All “lists” created by the account;
- o. All information on the “Who to Follow” list for the account;
- p. All privacy and account settings;
- q. All records of Twitter searches performed by the account, including all past searches saved by the account;
- r. All information about connections between the account and third-party websites and applications;
- s. All information regarding accounts linked by cookies to the accounts

described in Attachment A;

- t. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

Twitter is hereby ordered to disclose the above information to the government within 14 of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 2251 (sexual exploitation of children), 2252 (transportation, receipt, distribution and possession of material involving sexual exploitation of minors), 2252A (transportation, receipt, distribution and possession of child pornography) and 2422 (coercion and enticement) involving CARMINE SIMPSON since March 19, 2020, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- a. communications with minors and potential minors relating to the production and attempted production of child pornography, including those that evidence an effort to identify, groom and have any sexual relationship—virtually or physically with them;
- b. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the

Twitter account owner;

- c. Evidence indicating the Twitter account owner's state of mind as it relates to the crime under investigation;
- d. The identity of the person who created or used the user ID, including records that help reveal the whereabouts of such person.
- e. The identity of the persons who communicated with the user ID about matters relating to the production and attempted production of child pornography, including efforts to identify, groom and have any sexual relationship—virtually or physically—with minor victims, including records that help reveal their whereabouts.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.